Data security and encryption in low-power Wireless Sensor Networks

Ioan Deaconu
Automatic Control and Computers Faculty
University Politehnica of Bucharest,
{ioan.deaconu@cti.pub.ro}

The fist two pages are intended for grading.

I. Introduction

Wireless Sensors are low cost, low power devices optimized to perform custom tasks. They usually gather information from their surroundings and then send it to a base station server in order to be stored and processed. This communication is generally achieved using gateways. A gateway is usually connected to a more powerful device that can process the received information and take certain actions based on the results. The information transmitted by wireless sensors often represents sensitive data. For this reason, security protocols are implemented to prevent attacks that can intercept, replicate or alter the data.

Currently, security protocols in wireless sensor networks rely mostly on key based encryption algorithms. While this method can achieve great efficiency in terms of data security and protection, it also requires a certain level of computational power and is not always a task which is quickly executed. More so, in order to use such protocols, nodes must store all the necessary keys. Due to their design, wireless sensors often do not possess the necessary resources. They seldom have external memories attached to them and their processing power is limited to microprocessors which run at frequencies in the range of 1-20 MHz.

Another limitation of using this type of protocols to encrypt data is related to energy consumption. Usually, these sensors are powered by small batteries with a limited capacity. If the microprocessor has to perform intensive computations, these batteries will be drained in short amounts of time. Even equipping sensors with energy harvesting peripherals does not ensure that the battery lifespan is greatly increased.

The approach presented in this paper attempts to implement a more simple encryption algorithms which, combined with hardware encryption methods, can achieve an acceptable level of data security while ensuring that power consumption is kept to a minimum.

The proposed method relies on using available hardware AES ECB encryption in inter node communication and AES CBC for securing data.

This approach tries to find the balance point in the trade-off between security and energy consumption. While the data might not be protected as well as when key based algorithms are used, the energy consumption will be minimized thus increasing the life span of the sensor.

II. Related Work

Security is of prime importance in Wireless Sensor Networks. Nodes transfer important data between them and the cost of checking the validity and integrity of the transmitted packages is high, both from the energy consumption perspective as well as the necessary computational power perspective.

Possible attacks that might hinder the activity and integrity of a Wireless Sensor Network include:

- Wormhole attack: the attacker sends the received messages from one part of the network in a different part of the network. As a result, the nodes from both areas consider that the other nodes are neighbours and vice-versa.
- Blackhole/Sinkhole attack: the attackers makes itself more appealing from a routing point of view in order to receive all the messages from the network.
- Sybil attack: the attacker assumes the identity of one or more valid sensors[6].
- Selective forwarding attack: the attacker is able to intercept messages and drop certain packets or forward them [3].
- Hello Flood Attack: the attacker uses "HELLO" packets to flood its neighbors in order to force the nodes to trust him.

No current security framework available for Wireless Sensor Networks offers complete protection against all types of attacks. However they offer protection against specific attacks. All of the following implementations rely on software encryption methods:

- SPINS - 2002 - The communication parties create independent keys for encryption and decryption and MAC keys for communication. It provides security against Data and Information Spoofing and Message Replay Attacks[7].

- LEAP - 2003 - The protocol implies that the nodes exchange more than one type of message between them.Thus, the framework uses 4 different keys. It provides security against "HELLO" flood attacks, Sybil attacks and minimizes the consequences of spoofing, altering, replay routing information and selective forwarding attacks [9].
- TinySec - 2004 - The key is pre-deployed on the node, but it does not provide any solution for changing the key. If a node is compromised, the entire network will be compromised. It provides security against Data and Information Spoofing and Message Replay Attacks [4].
- LEAP+ - 2006 - It uses the same idea as LEAP, but the overhead is reduced. It provides security against Confidentiality and authentication, "HELLO" flood attacks, Sybil attacks and minimizes the consequences of spoofing, altering, replay routing information and selective forwarding attacks [9].
- MiniSec - 2007 - Uses a counter IV mechanism. The counter is incremented locally and only the last bits of the counter are sent. It provides security against Authentication, Data Secrecy and Reply Attack [5].
- pDCS - 2009 - It uses 5 different keys to achieve data security. It provides security against Location and Query privacy [8].
- TinyKey - 2011 - An improvement of TinySec. It adds the key management system, in order to be able to change the key after the node is deployed. It provides security against Message authentication, confidentiality and integrity [1].
- ERP-DCS - 2013 - It proposes a different way of creating and storing keys when compared with pDCS. It provides security against Location and Query privacy [2].

III. Architecture

A. Hardware

The processing power and wireless capability of the wireless sensor nodes are provided by an Atmel ZigBit 900MHZ RF module. It contains an ATmega 1281V 8-bit microcontroller connected to an AT86RF212 RF Transceiver via a SPI interface. The Atmega 1281V is an low power 8 bit microcontroller that is connected to the onboard sensors of the node. In order to be able to transmit or secure the data, the microcontroller will communicate with the RF Transceiver. The Transceiver controller is a very low power chip, capable of sending data up to 6 km. Also, the Transceiver contains a security module compatible with AES-128. It supports hardware encryption and decryption for AES 128 ECB, but but for the AES 128 CBC it is available only the hardware encryption.

B. Software

From the software perspective, the architecture is composed of three modules:

- data module, that collects information from the sensors,

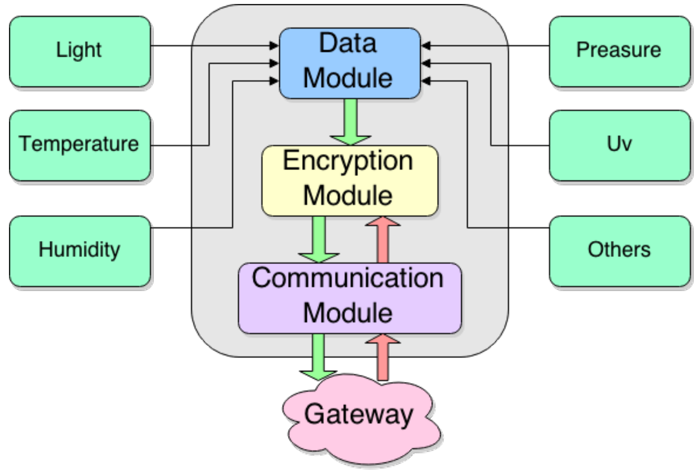

Figure 1. System Architecture

- encryption module,
- communication module.

The main focus on this paper will be placed on the encryption module. The encryption method for the data uses the two supported hardware methods: AES 128 ECB and AES 128 CBC. It is necessary to use both of them because the nodes are transmitting two kinds of packets: a first type of packets which contains non-sensitive data and is used by the receiver to identify the sender and a second type of packets which contains the actual sensitive data. Since it supports both encryption and decryption, the first set of packets, those containing identification information, are encrypted using ECB. The data itself is encrypted using CBC. Since CBC decryption is not supported by default, a software CBC decryption implementation is necessary in order to allow the sensors to verify the data at regular intervals.

In addition to the CBC decryption, it is also required to have implementations of other software encryption algorithms in order to perform the performance analysis. The chosen algorithms which will be used in benchmarking are Skipjack and RC5.

References

[1] R. Doriguzzi Corin, G. Russello, and E. Salvadori. Tinykey: A light-weight architecture for wireless sensor networks securing real-world applications. In *Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on*, pages 68–75. IEEE, 2011.

[2] J.-M. Huang, S.-B. Yang, and C.-L. Dai. An efficient key management scheme for data-centric storage wireless sensor networks. *IERI Procedia*, 4:25–31, 2013.

[3] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 335–340. IEEE, 2007.

[4] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.

[5] M. Luk, G. Mezzour, A. Perrig, and V. Gligor. Minisec: a secure sensor network communication architecture. In *Proceedings of the 6th international conference on Information processing in sensor networks*, pages 479–488. ACM, 2007.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[8] M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang. pdcs: Security and privacy support for data-centric sensor networks. *Mobile Computing, IEEE Transactions on*, 8(8):1023–1038, 2009.

[9] S. Zhu, S. Setia, and S. Jajodia. Leap+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(4):500–528, 2006.